+357 96 030922
info@marketpublishers.com

Post-Quantum Cryptography Market Forecasts to 2034 – Global Analysis By Offering (Solutions and Services), Algorithm Type, Deployment Mode, End User and By Geography

https://marketpublishers.com/r/P30465274F80EN.html
Date: April 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: P30465274F80EN

Abstracts

According to Stratistics MRC, the Global Post-Quantum Cryptography Market is accounted for $0.7 billion in 2026 and is expected to reach $19.2 billion by 2034, growing at a CAGR of 49.5% during the forecast period. Post-Quantum Cryptography (PQC) is a field of cryptography focused on developing encryption methods capable of resisting attacks from quantum computers. Traditional cryptographic systems may become vulnerable once large-scale quantum computing becomes practical. PQC uses mathematical problems that are considered difficult for both classical and quantum computers to solve. These algorithms are designed to run on existing computing systems and communication networks while providing protection against quantum-based threats, ensuring that sensitive data and digital communications remain secure in the future.

Market Dynamics:

Driver:

Growing threat of quantum decryption

Quantum machines using Shor’s algorithm can theoretically break these protocols within hours, exposing global digital infrastructure. Governments and enterprises are accelerating PQC adoption to safeguard sensitive data against future harvest-now-decrypt-later attacks. Increasing investments in national quantum initiatives and post-quanture roadmaps are compelling organizations to upgrade cryptographic assets. The

+357 96 030922
info@marketpublishers.com

urgency is further amplified by data retention regulations, as stolen encrypted data today could be decrypted by future quantum systems, making proactive migration to PQC a strategic imperative for long-term security.

Restraint:

High migration complexity and costs

Transitioning from classical to post-quantum cryptography involves overhauling legacy systems, hardware modules, and communication protocols. Enterprises face significant technical challenges in integrating PQC algorithms without disrupting existing operations. Smaller organizations struggle with the financial burden of cryptographic audits, staff retraining, and system upgrades. Additionally, hybrid cryptographic modes that run classical and PQC algorithms in parallel demand higher computational resources. These constraints slow down mass adoption, particularly in industries with legacy-dependent operational technology environments.

Opportunity:

Government mandates and compliance requirements

Regulatory bodies worldwide are issuing guidelines and deadlines for quantum-safe migration. The U.S. National Institute of Standards and Technology (NIST) has finalized PQC standards, while the EU and other regions are developing similar frameworks. Compliance with directives such as the EU Cybersecurity Act and U.S. Quantum Computing Cybersecurity Preparedness Act is forcing public and private sectors to adopt PQC solutions. This regulatory push creates a multi-billion-dollar opportunity for vendors offering migration tools, consulting, and managed services. Early adopters gain competitive advantage by demonstrating quantum readiness, while technology providers can bundle PQC with existing security suites to accelerate market penetration.

Threat:

Immature standards and algorithm vulnerabilities

Although NIST has standardized several PQC algorithms, the field remains relatively young compared to classical cryptography. New cryptanalysis techniques continue to uncover potential vulnerabilities in lattice-based, code-based, and multivariate schemes. The risk of undiscovered backdoors or mathematical weaknesses poses a serious

+357 96 030922
info@marketpublishers.com

threat to long-term trust in PQC solutions. Furthermore, hardware acceleration for PQC is not yet widespread, leading to latency issues in high-throughput environments. Organizations may delay adoption until algorithms mature further, creating a window of exposure. Without continuous monitoring and agile cryptographic agility, early adopters could face costly re-migrations if selected algorithms are compromised.

Covid-19 Impact

The pandemic accelerated digital transformation, expanding attack surfaces across remote work, telehealth, and cloud services. This surge in data exchange heightened awareness of long-term cryptographic risks, including quantum threats. However, budget reallocations toward immediate pandemic response delayed some PQC research and pilot projects. Supply chain disruptions affected hardware security module availability for cryptographic testing. Conversely, government stimulus packages included cybersecurity modernization funds, indirectly supporting PQC readiness. Post-pandemic strategies now emphasize cryptographic agility, with organizations integrating PQC into zero-trust architectures and long-term data protection plans, recognizing quantum resilience as a critical business continuity factor.

The solutions segment is expected to be the largest during the forecast period

The solutions segment is expected to account for the largest market share, driven by immediate demand for quantum-resistant encryption tools, key management systems, and secure communication platforms. Enterprises are prioritizing software libraries and hardware modules that replace vulnerable RSA and ECC implementations. Encryption tools enable data-at-rest and in-transit protection, while key management ensures secure cryptographic lifecycle governance. Digital signatures based on PQC algorithms prevent forgery in legal and financial transactions.

The BFSI segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the BFSI segment is predicted to witness the highest growth rate, driven by the need to protect long-lived financial data, transaction integrity, and payment systems. Banks and insurance firms face significant risks from harvest-now-decrypt-later attacks on wire transfers, customer records, and blockchain assets. Regulatory pressure from central banks and financial authorities is accelerating PQC pilots and migrations. Integration of quantum-safe algorithms into ATMs, online banking platforms, and interbank settlement systems is rising.

+357 96 030922
info@marketpublishers.com

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, fuelled by aggressive government initiatives from NIST and the Department of Homeland Security. The United States leads in PQC standardization, research funding, and early adoption across defense, finance, and cloud sectors. Presence of major technology vendors and cryptographic startups accelerates product commercialization. Strong collaboration between national labs, universities, and private enterprises drives algorithm development and testing.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, supported by rapid digitalization and growing quantum computing research in China, Japan, India, and South Korea. Governments are launching national quantum missions and post-quantum migration roadmaps to protect critical infrastructure. Increasing cross-border data flows and cyber threats from state-sponsored actors drive urgency for PQC adoption. Expanding BFSI, telecom, and e-commerce sectors seek quantum-safe solutions for long-term data protection.

Key players in the market

Some of the key players in Post-Quantum Cryptography Market include IBM Corporation, Microsoft Corporation, Amazon Web Services, NXP Semiconductors, Thales Group, IDEMIA, Palo Alto Networks, DigiCert, PQShield, Post?Quantum Ltd., ISARA Corporation, QuintessenceLabs, Quantum Xchange, Keyfactor, and QuSecure.

Key Developments:

In March 2026, IBM and ETH Zurich announced a 10-year collaboration to advance the next generation of algorithms at the intersection of AI and quantum computing. This initiative represents the latest milestone in the long-standing collaboration between the two institutions, further strengthening a scientific exchange that has helped create the future of information technology.

In March 2026, Thales partners with Service Oklahoma to launch next-generation driver licenses and ID cards. Service Oklahoma has selected Thales to deliver new driver licenses and ID cards designed for maximum security, durability, and sustainability. The new credentials are made from 100% polycarbonate, a durable material that embeds

+357 96 030922
info@marketpublishers.com

advanced security features to prevent fraud.

Offerings Covered:

- Solutions
- Services

Algorithm Types Covered:

- Lattice- based
- Code? based
- Multivariate
- Hash? based
- Isogeny? based

Deployment Modes Covered:

- On?Premises
- Cloud

End Users Covered:

- BFSI
- Government & Defense
- IT & Telecom
- Healthcare

+357 96 030922
info@marketpublishers.com

- Retail & eCommerce
- Manufacturing
- Energy & Utilities
- Other End Users

Regions Covered:

- North America
  - United States
  - Canada
  - Mexico
- Europe
  - United Kingdom
  - Germany
  - France
  - Italy
  - Spain
  - Netherlands
  - Belgium
  - Sweden
  - Switzerland

+357 96 030922
info@marketpublishers.com

- Poland
- Rest of Europe

Asia Pacific

- China
- Japan
- India
- South Korea
- Australia
- Indonesia
- Thailand
- Malaysia
- Singapore
- Vietnam
- Rest of Asia Pacific

South America

- Brazil
- Argentina
- Colombia
- Chile
- Peru

+357 96 030922
info@marketpublishers.com

- Rest of South America
- Rest of the World (RoW)
  - Middle East
    - Saudi Arabia
    - United Arab Emirates
    - Qatar
    - Israel
    - Rest of Middle East
  - Africa
    - South Africa
    - Egypt
    - Morocco
    - Rest of Africa

What our report offers:

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)

+357 96 030922
info@marketpublishers.com

- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

- Company Profiling
  - Comprehensive profiling of additional market players (up to 3)
  - SWOT Analysis of key players (up to 3)
- Regional Segmentation
  - Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)
- Competitive Benchmarking
  - Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

9 GLOBAL POST-QUANTUM CRYPTOGRAPHY MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Post-Quantum Cryptography Market Forecasts to 2034 – Global Analysis By Offering (Solutions and Services), Algorithm Type, Deployment Mode, End User and By Geography

Product link: https://marketpublishers.com/r/P30465274F80EN.html

Price: US$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/P30465274F80EN.html